REMARKS

Claims 1-26 and 30 are currently pending in the subject application and are presently under consideration. Claims 1, 3, 4, 16, 22, 26, and 30 have been amended as shown at pp. 2-8 of the Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-20, 22-26 and 30 Under 35 U.S.C §112

Claims 1-20, 22-26 and 30 stand rejected under 35 U.S.C §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention. Claims 1, 16, 22, 26 and 30 have been amended to cure any deficiencies related this rejection. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 1-26 and 30 Under 35 U.S.C. §103(a)

Claims 1-26 and 30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Hadfield *et al.* (Lee Hadfield, Dave Heller, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN 078971213) in view of Lloyd *et al.* (U.S. Patent 6219790) and further in view of Kaeo (Merike Kaeo, "Designing network Security", 1999, ISBM: 1578700434). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Hadfield *et al.*, Lloyd *et al.*, and Kaeo, alone or in combination, do not teach or suggest each and every limitation of applicants' claimed invention.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found

in the prior art and not based on applicants' disclosure. *See In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The subject invention relates to responding to challenges from various authentication systems that does not require recompiling and recoding of an application making the access request in an environment where the authentication systems are changing. For instance, applicants' claimed invention can receive an authentication challenge and send first data to an authentication manager that contains the challenge data minus any communication protocol data. This allows for an authentication manager that is generic for various communication protocols. The authentication manager can process the first data into one or more second data and pass the second data to one or more authentication modules. The ability for the authentication manager to produce multiple types of second data allows for the authentication manager to interact with various authentication modules that require differing input data. The second data can be specific to the needs of the authentication module that the second data is being sent to, such as by adding to, transforming, or removing some of the first data. In the case where the authentication module needs to interact with multiple authentication modules for a challenge, the authentication manager can process the first data into second data for one authentication module and different second data for another authentication module.

In particular, claim 1 (and similarly independent claims 16, 22, 26 and 30) recites *an authentication manager that receives first data associated with the communication challenge* ***and processes the first data into second data of a first type appropriate for a first authentication module, the authentication manager further processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for secondary data,*** *the authentication manager further communicates at least one of the second data to at least one authentication module, the second data related to the first data and the authentication challenge.*

As conceded in the Office Action, Hadfield *et al.* fails to teach that the authentication manager further processes the first data into second data of a second type appropriate for a second authentication module. The Examiner cites Lloyd *et al.* to make up for this deficiency of Hadfield *et al.* However, Lloyd *et al.* merely indicates that multiple authentication protocols/modules are supported. The cited art makes no suggestion that a single authentication

request from a client will be converted into to sets of data for two different authentication modules to complete the single authentication request. Lloyd *et al.* clearly indicates that a single authentication protocol is derived from a server name in the login username or from a default server listed in a data table, and then the appropriate authentication module is used.

Furthermore, Kaeo teaches receipt of a challenge message containing challenge data. The challenge data is sent to a hashing function minus any communication protocol data to produce a response. Therefore, Kaeo, also fails to teach or suggest processing the challenge data into two different data *prior* to employing the hashing function, which is where the authentication takes place.

In view of at least the foregoing comments, it is readily apparent that the cited art, alone or in combination, provide no suggestion that an authentication manager receives first data associated with the communication challenge and processes the first data into second data of a first type appropriate for a first authentication module, the authentication manager further processes the first data into second data of a second type appropriate for a second authentication module, the first and second authentication modules having different requirements for secondary data as in applicants' claimed invention.

Hadfield *et al.*, Lloyd *et al.*, and Kaeo, alone or in combination, do not teach or suggest applicants' invention as recited in independent claims 1, 16, 22, 26 and 30 (and claims 2-15, 17-21 and 23-25 which respectively depend there from). Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP202US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN & TUROCY, LLP

Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731